Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (Original): An authentication apparatus, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an estimation unit estimating matching precision of the extracted biometric feature information;

a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

an authentication unit information input unit inputting the authentication information;

a biometric feature information registration unit preliminarily storing registered biometric feature information;

an authentication information registration unit preliminarily storing additional registered authentication information;

a biometric feature information matching check unit having a matching check between the extracted biometric feature information and the registered biometric feature information;

an authentication information matching check unit having a matching check between the input authentication information and the registered authentication information; and

a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication

information, and determining based on a computation result whether or not a user is authenticated.

Claim 2 (Original): The apparatus according to claim 1, wherein

said request unit requests password information as the authentication information, said authentication information input unit inputs the password information, said authentication information registration unit preliminarily stores registered password information as the registered authentication information, and said authentication information matching check unit has a matching check between the input password information and the registered password information.

Claim 3 (Original): The apparatus according to claim 2, wherein

said request unit comprises a setting unit setting a number of digits of password information required to obtain the predetermined matching precision, and requesting an input of the set number of digits of password information.

Claim 4 (Original): The apparatus according to claim 3, wherein

said number of digits is set based on the matching precision estimated by said estimation unit, and said authentication information matching check unit has a matching check between the input password information and a predetermined part of the registered password information.

Claim 5 (Original): The apparatus according to claim 1, wherein said determination unit inputs authentication information stored in a medium.

Claim 6 (Original): An authentication apparatus, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an estimation unit estimating matching precision of the extracted biometric feature information;

a request unit requesting an input of other biometric information when it is estimated that predetermined matching precision cannot be obtained;

a biometric feature information registration unit preliminarily storing plural pieces of registered biometric feature information;

a biometric feature information matching check unit having a matching check between the extracted biometric feature information and the registered biometric feature information; and

a determination unit computing matching precision by combining matching check results about the plural pieces of biometric feature information extracted from plural pieces of input biometric information, and determining based on a computation result whether or not a user is authenticated.

Claim 7 (Original): The apparatus according to claim 6, wherein

said request unit requests an input of other biometric information of a same type as the biometric information used in estimating matching precision, and said biometric information input unit inputs other biometric information of the same type at the request.

Claim 8 (Original): The apparatus according to claim 7, wherein

said biometric input unit inputs fingerprint information as biometric information, and requests an input of fingerprint information about a finger different from a finger used in fingerprint information in a matching check for estimating the matching precision.

Claim 9 (Original): The apparatus according to claim 6, wherein

said request unit requests an input of biometric information of a different type from biometric information used in estimating matching precision, and said biometric information input unit inputs biometric information of a different type.

Claim 10 (Original): An authentication apparatus, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an authentication information input unit inputting additional authentication information;

a biometric feature information registration unit preliminarily storing registered biometric feature information;

an authentication information registration unit preliminarily storing additional registered authentication information;

a biometric feature information matching check unit having a matching check between the extracted biometric feature information and the registered biometric feature information;

an authentication information matching check unit having a matching check between the input authentication information and the registered authentication information when the predetermined matching precision cannot be obtained from the matching check result about the biometric feature information; and

a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and determining based on a computation result whether or not a user is authenticated.

Claim 11 (Original): The apparatus according to claim 10, wherein

said biometric information relates to one of fingerprint information, iris information, voiceprint information, retina blood vessel distribution information, signature information, face image information, and DNA information.

Claim 12 (Original): A client device in a client-server type authentication system, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an estimation unit estimating matching precision of the extracted biometric feature information;

a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

an authentication information input unit inputting the authentication information;

a generation unit generating matching check data by combining the extracted biometric feature information with the input authentication information; and

a communications unit transmitting the matching check data to a server to have a matching check between the generated matching check data and registered information.

Claim 13 (Original): The apparatus according to claim 12, wherein

said matching data generation unit described in the matching data at least one of the extracted biometric feature information, type information about the input authentication information, and format information about the matching data device.

Claim 14 (Original): A server device in a client-server type authentication system, comprising:

a communications unit receiving biometric feature information and additional authentication information from a client;

a biometric feature information registration unit preliminarily storing registered biometric feature information;

an authentication information registration unit preliminarily storing additional registered authentication information;

a biometric feature information matching check unit having a matching check between the received biometric feature information and the registered biometric feature information;

an authentication information matching check unit having a matching check between the received authentication information and the registered authentication information; and

a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and determining based on a computation result whether or not a user is authenticated.

Claim 15 (Original): An authentication apparatus, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an estimation unit estimating matching precision of the extracted biometric feature information;

a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

an authentication information input unit inputting the authentication information;

a biometric feature information registration unit storing the biometric feature information as registered biometric feature information;

an authentication information registration unit storing the authentication information as additional registered authentication information;

a biometric feature information matching check unit having a matching check between biometric feature information extracted from the biometric information input for authentication and registered biometric feature information;

a1

an authentication information matching check unit having a matching check between the authentication information input for authentication and the registered authentication information; and

a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about the additional authentication information, and determining based on a computation result whether or not a user is authenticated.

Claim 16 (Original): A client device in a client–server type authentication system, comprising:

a biometric information input unit inputting biometric information;

an extraction unit extracting biometric feature information from the input biometric information;

an estimation unit estimating matching precision of the extracted biometric feature information;

a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

an authentication information input unit inputting the authentication information;

a generation unit generating registration data by combining the extracted biometric feature information with the input authentication information; and

a communications unit transmitting the registration data to a server to register the generated registration data.

Claim 17 (Original): A serve device in a client-server type authentication system, comprising:

a communications unit receiving biometric feature information and additional authentication information from a client;

a biometric feature information registration unit storing the received biometric feature information as registered biometric feature information;

an authentication information registration unit storing the received authentication information as additional registered authentication information;

a biometric feature information matching check unit having a matching check between the biometric feature information received from a client for authentication and the registered biometric feature information;

an authentication information matching check unit having a matching check between the authentication information received from the client for authentication and the registered authentication information; and

a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and determining based on a computation result whether or not a user is authenticated.

Claim 18 (Original): The apparatus according to claim 17, further comprising:

a database unit managing a type of registered information stored corresponding each of piece identification information;

a retrieval unit retrieving a type of registered information corresponding to identification received from a client; and

a request unit requesting the client to input matching information corresponding to the retrieved type.

Claim 19 (Original): An authenticating method, comprising:

obtaining biometric information;

extracting biometric feature information from the received biometric information;

estimating matching precision of the extracted biometric feature information;

obtaining additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

having a matching check between the extracted biometric feature information and preliminarily registered biometric feature information;

having a matching check between the obtained authentication information and the preliminarily registered additional authentication information; and

computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and determining based on a computation result whether or not a user is authenticated.

Claim 20 (Currently Amended): An authentication apparatus, comprising:

biometric information input ~~measn~~ means for inputting biometric information;

extraction ~~measn~~ means for extracting biometric feature information from the input biometric information;

estimation ~~measn~~ means for estimating matching precision of the extracted biometric feature information;

request ~~measn~~ means for requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained;

authentication information input ~~measn~~ means for inputting the authentication information;

biometric feature information registration ~~measn~~ means for preliminarily storing registered biometric feature information;

authentication information registration ~~measn~~ means for preliminarily storing additional registered authentication information;

biometric feature information matching check ~~measn~~ means for having a matching check between the extracted biometric feature information and the registered biometric feature information;

authentication information matching check ~~measn~~ means for having a matching check between the input authentication information and the registered authentication information; and

determination ~~measn~~ means for computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and for determining based on a computation result whether or not a user is authenticated.